악성코드 지역화 – 국내환경과 악성코드

2010.8.30

㈜ 안철수연구소
ASEC (AhnLab Security Emergency response Center)

Anti-Virus Researcher
차민석 선임 연구원 (jackycha@ahnlab.com)

목 차

1. 최근 악성코드 동향

2. 한국형 악성코드 등장

3. 한국형 악성코드 메시지

4. 국내 환경 장벽

5. 국내 환경 이용

6. 향후 전망

1. 최근 악성코드 동향

안철수연구소

1. 최근 악성코드 동향

- 금전적 이득 목적
- 정치 및 이념 목적 (정보전)

- 대량 살포
- 타겟 공격

- 지역화

-> 악성코드 제작자들의 금전적 이득 목적으로 2004년 악성코드 대량 살포와 2006년 이후 지역화 속에 한국적 상황을 이용하는 이른바 '한국형 악성코드' 대거 등장

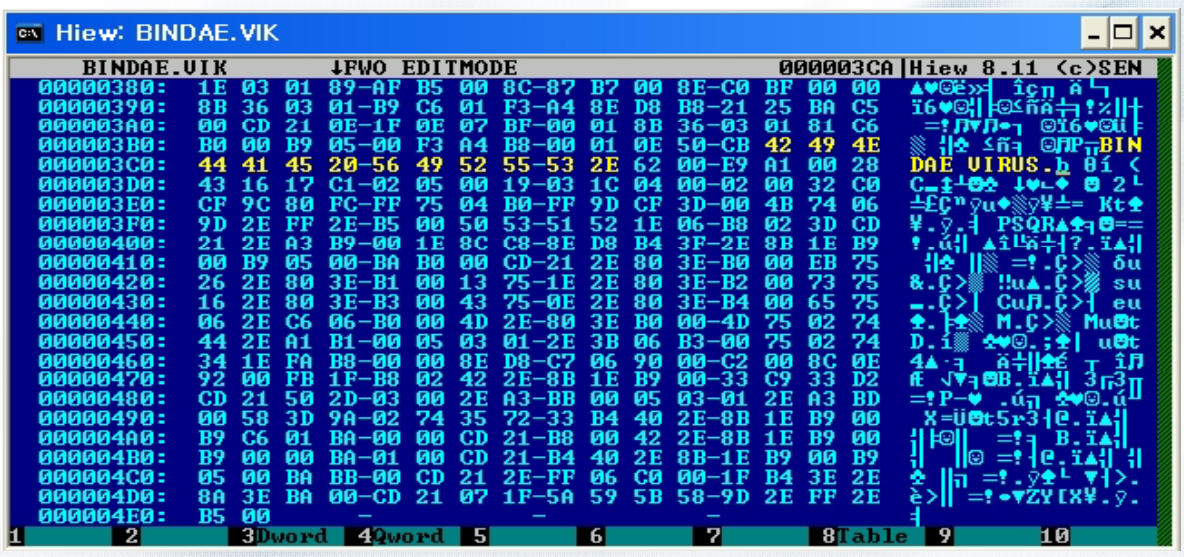
Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved.
안철수연구소

2. 한국형 악성코드 등장

안철수연구소

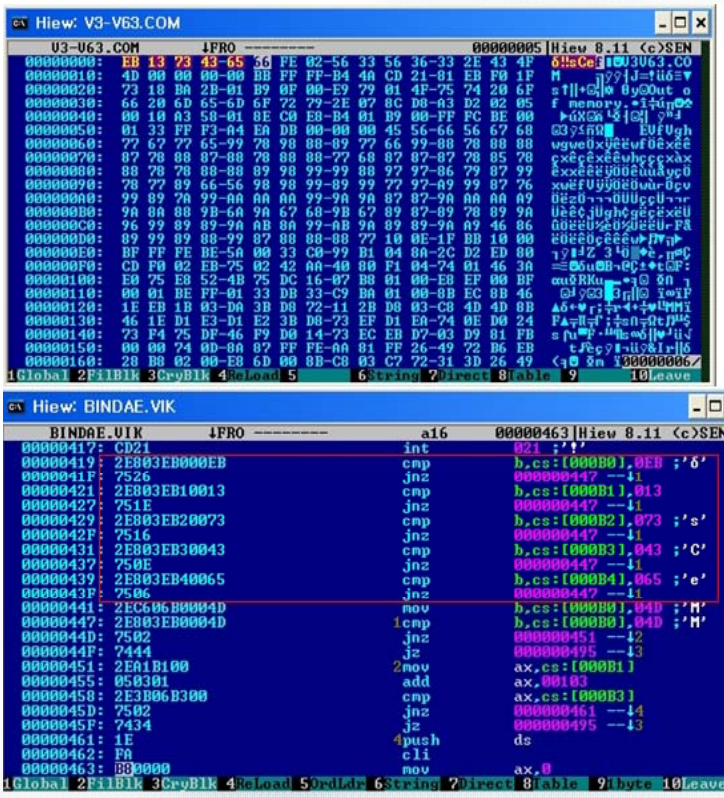
빈대 바이러스 (Bindae virus)

- 최초의 한국형 바이러스
- 1991년 5월 발견된 국산 도스 바이러스
- 13일의 금요일 'BINDAE VIRUS.' 메시지 출력
- 백신 III 프로그램 (V3.COM,V3RES.COM)을 감염시키지 않아 발견 시기를 늦춤
- 안철수 박사 : "분석하면서 놀라움이나 신기함보다는 슬픔이 앞섰다."



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved.

빈대 바이러스 (Bindae virus)



-V3는 신종 바이러스에 감염되었을 때 알려주는 기능 있음

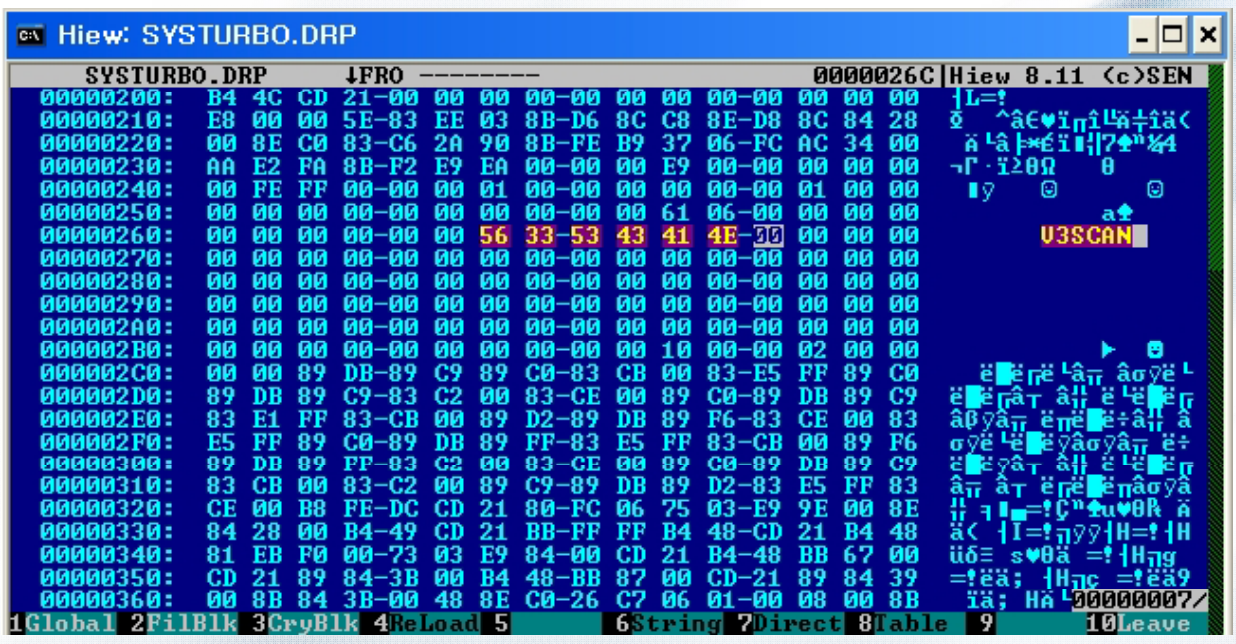
-외산 바이러스 제작자는 V3를 몰라 V3 파일을 감염시켜 쉽게 발견됨

- 빈대 바이러스는 V3 실행 파일과 동일하면 감염 시키지 않아 발견을 늦춤

Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

시스터보 바이러스 (Systurbo virus)

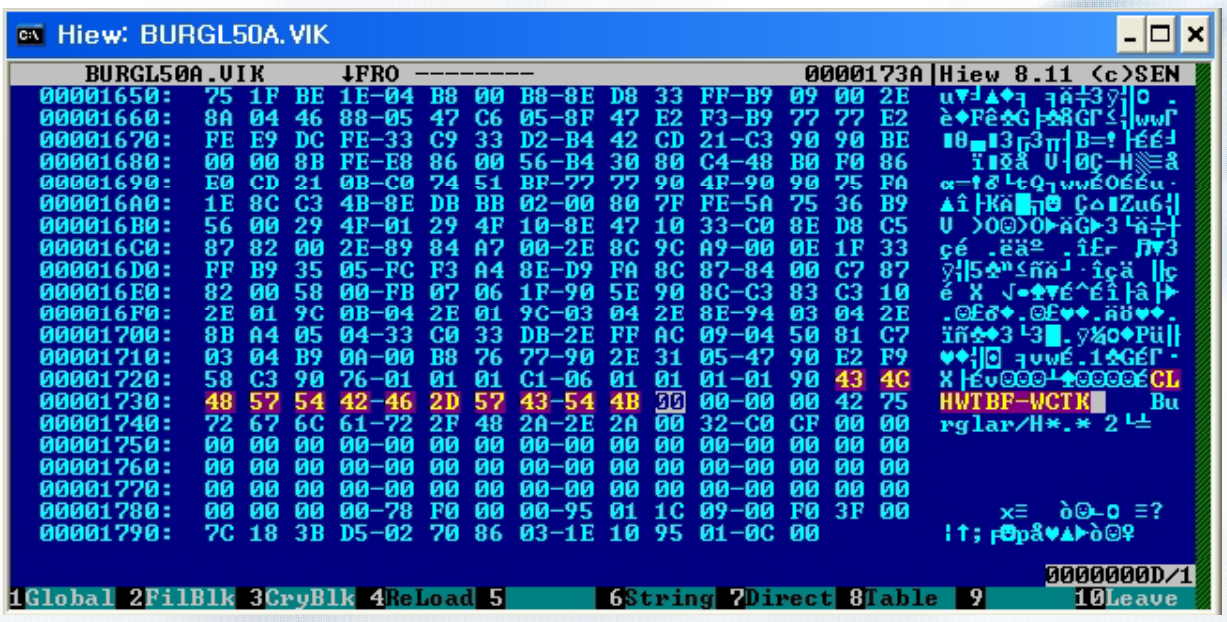
- 1994년 하이텔 자료실에서 발견된 국산 도스 바이러스
- V3와 SCAN 로 시작하는 파일을 감염시키지 않음
- 문자열 때문에 해외에서 V3scan라는 이름으로도 불임



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

강도.1150 바이러스 (Burglar.1150 virus)

- 1995년 발견된 국산 도스 바이러스
- 국내에서 널리 사용되는 자체 검사 기능 가진 파일(CL, HW, TB, F-, WC, TK)을 감염시키지 않음
- 파일 이름에 S나 V 가 포함된 파일도 감염시키지 않음

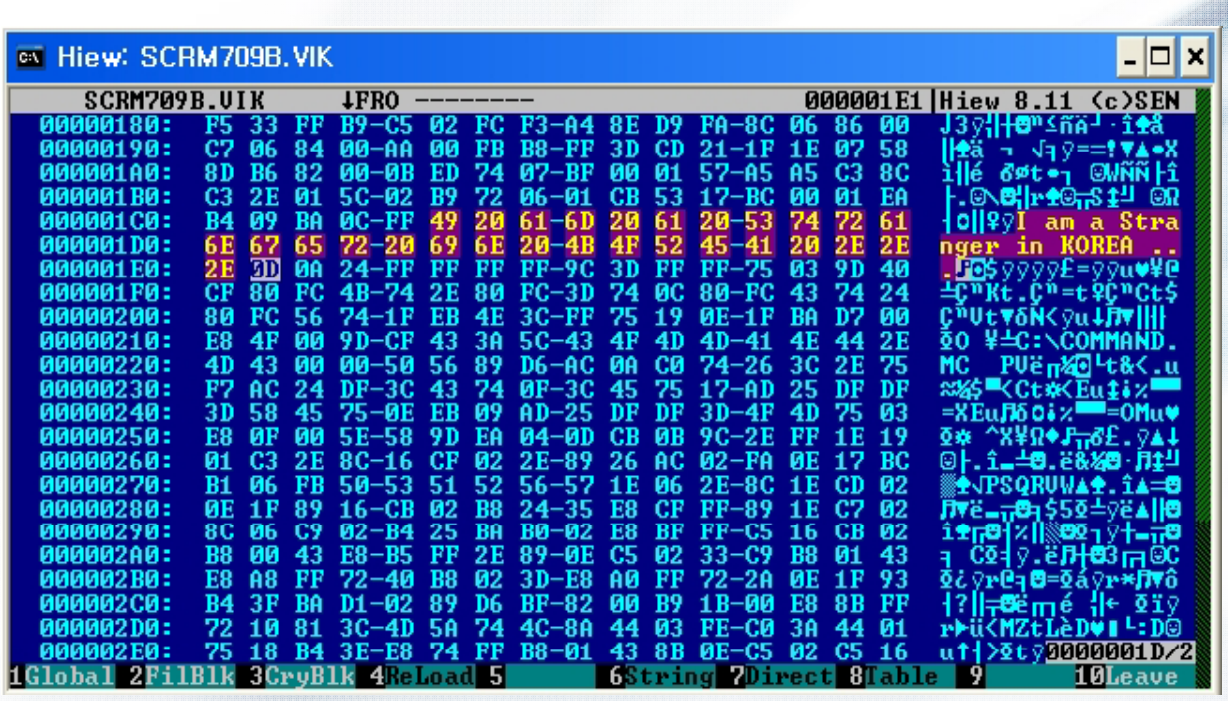


Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved.

3. 한국형 악성코드 메시지

한국산 표시

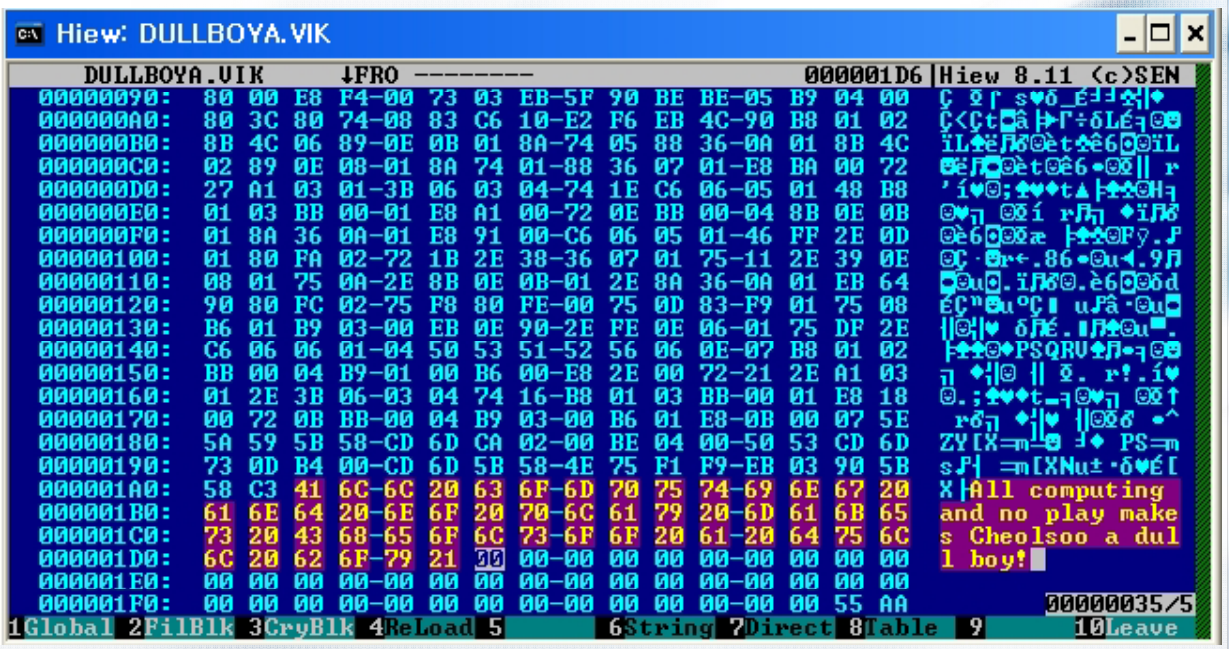
Scream.709.Kr virus
- 외산 바이러스를 변형한 반쪽 국산 바이러스



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

백신 제작자 조롱

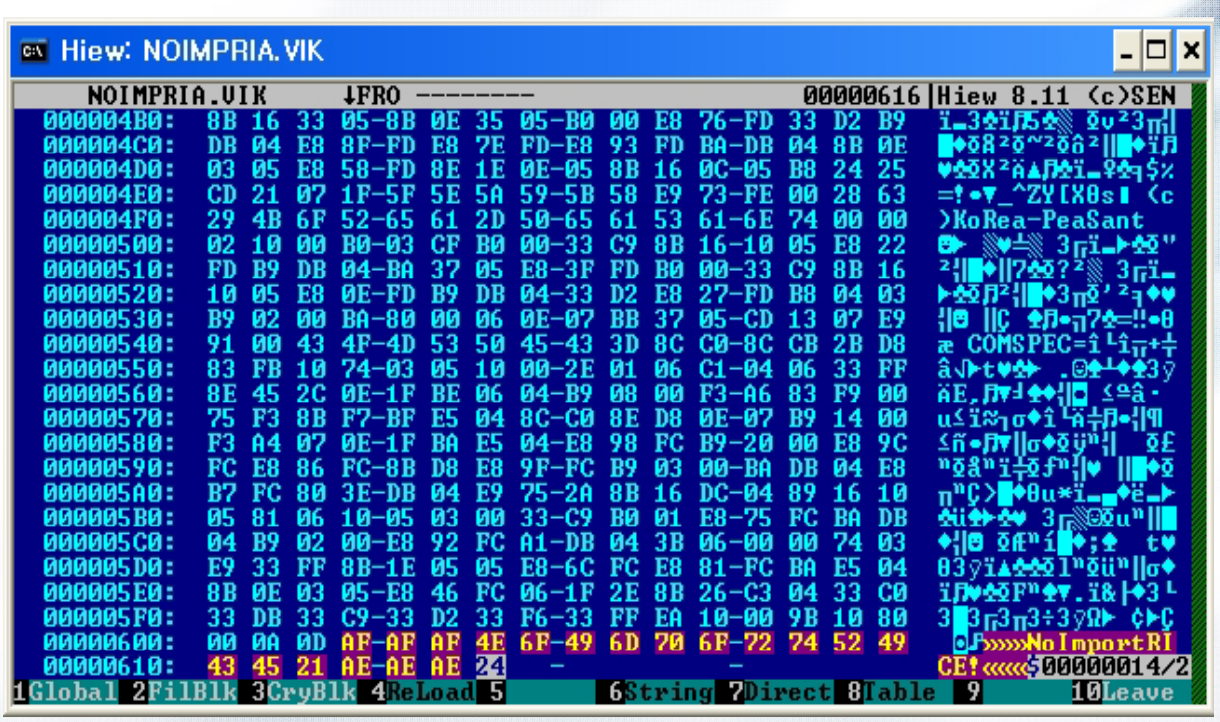
Dull_boy virus
- All computing and no play makes Cheolsoo a dull boy!
- 해외에서는 철수 바이러스로 불리기도 함



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

사회 문제

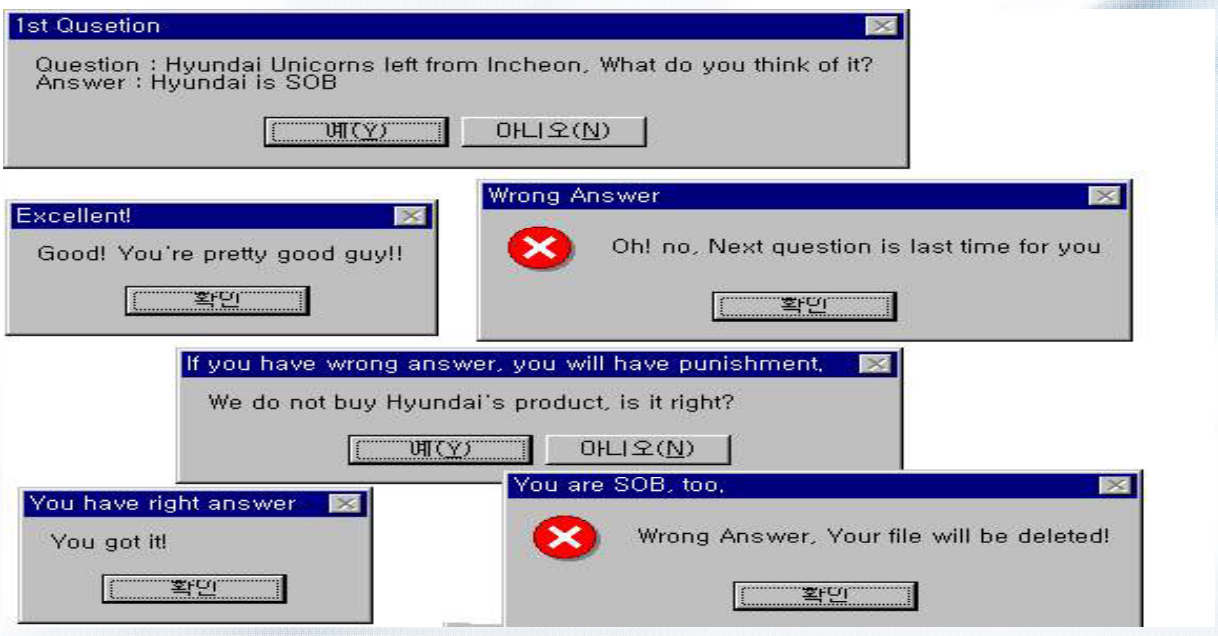
No_Import_Rice virus
- 1994년 쌀수입 반대 메시지 포함



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

개인적 불만

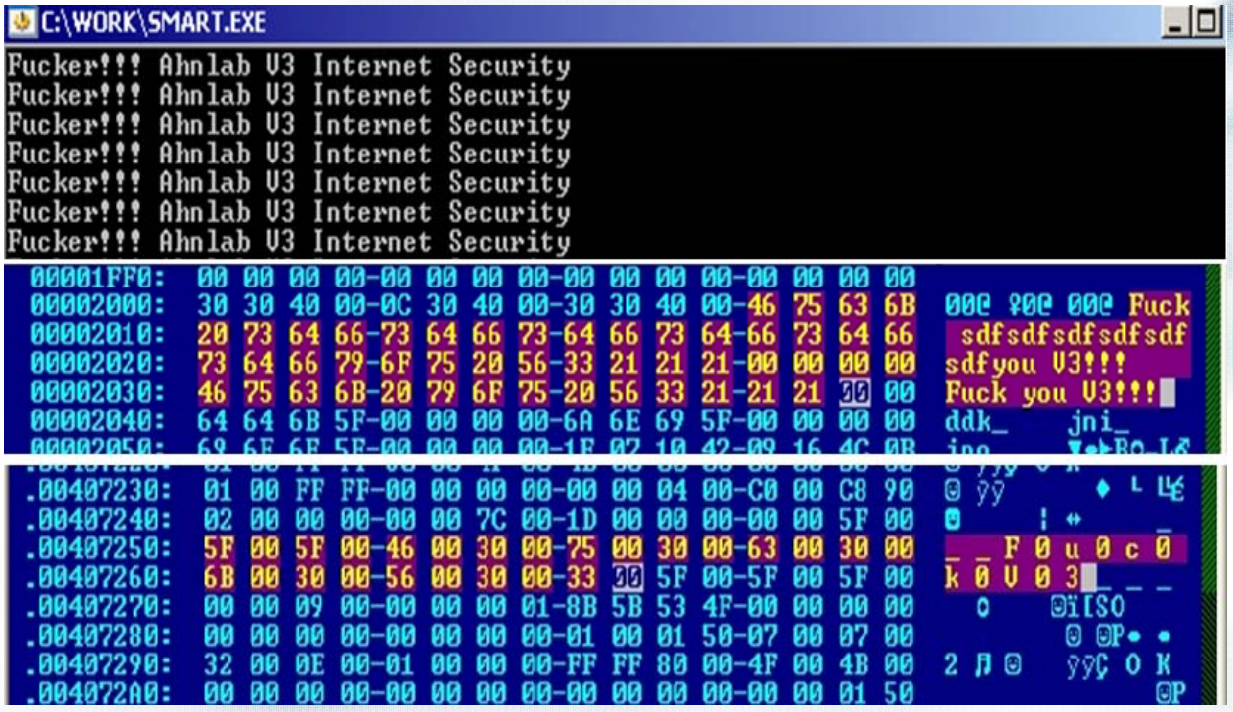
X97M/Hjb.I virus
- 2000년 인천을 떠나는 현대 유니콘와 현대에 대한 비난
- 매달 25일 사용자에게 질문 후 원하는 답이 아니면 현재 작업 문서 삭제



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

백신 욕설

- 자신들의 돈벌이를 방해하는 백신 회사 혹은 백신 프로그램에 대한 욕설

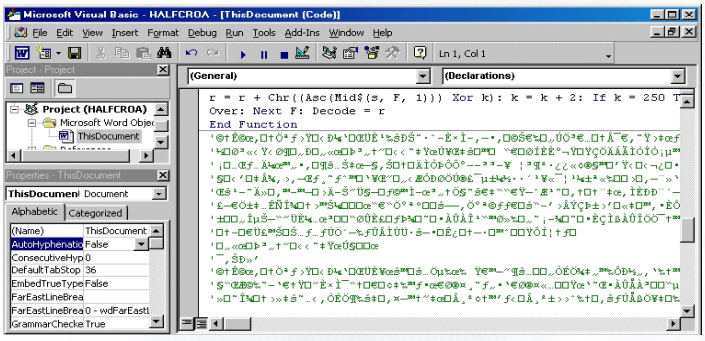


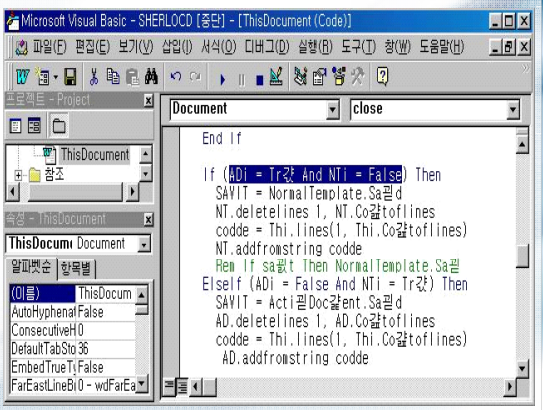
Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved.

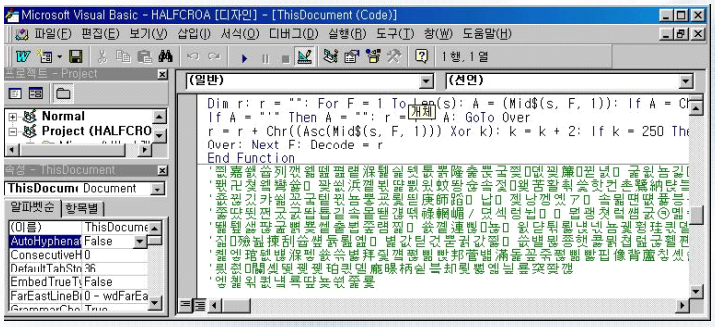
4. 국내 환경 장벽

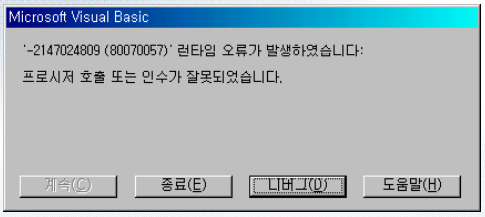
장벽 1. 언어

- 사용자들이 영문 메일은 잘 읽지 않음
- 한글 윈도우에서 오동작 하는 악성코드 존재





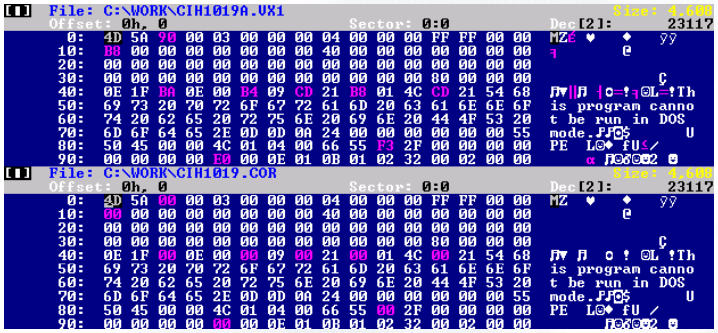


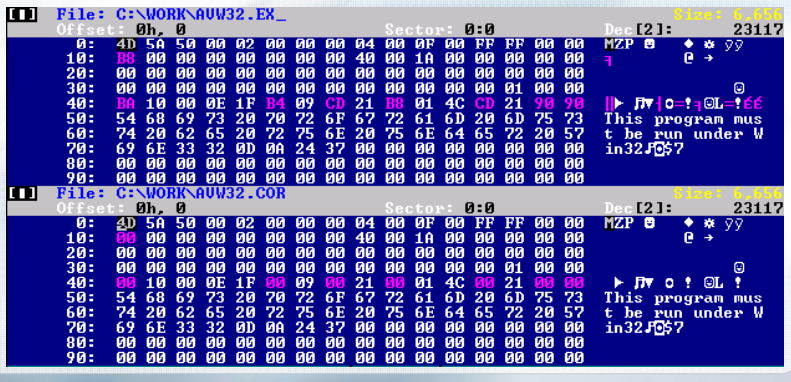


Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

장벽 1. 언어

- 한글 윈도우에서는 스크립트나 매크로에서 생성하는 파일 중 내용이 손상되어 실행 안될 수 있음





Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

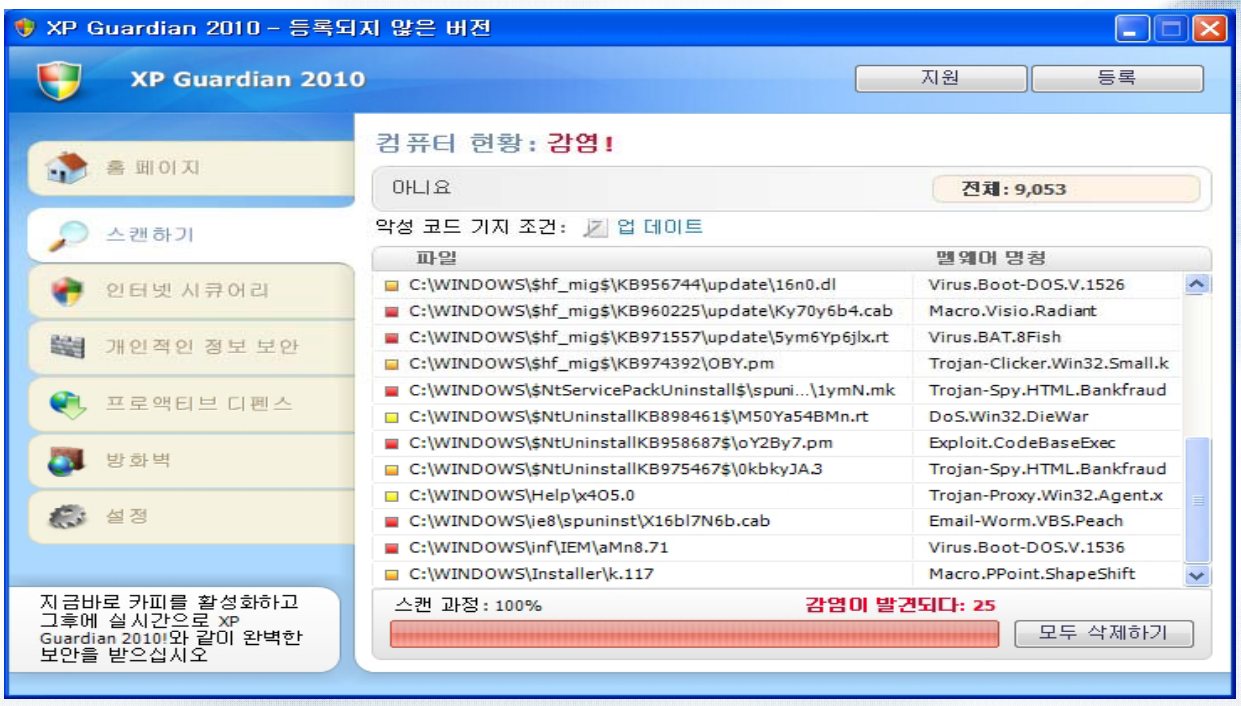
장벽 1. 언어 – 짧은 한글

- '안녕하세요! 90 아름다움 후' 같은 짧은 한글
- 인터넷 검색해서 긁어 옴 ?

Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

장벽 1. 언어 – 번역기

- 리소스를 번역기로 번역
- 아직은 조금 어색한 한글 -> 번역기 성능에 달림



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

장벽 1. 언어 – 한국어 가능자

- 한국어 가능자(조선족 등)의 보다 치밀한 메일
- 한국에서 사용하는 문법이나 표현과 다름
- 공격자 메일에는 '두음법칙' 무시
- 주로 타겟 공격에 이용

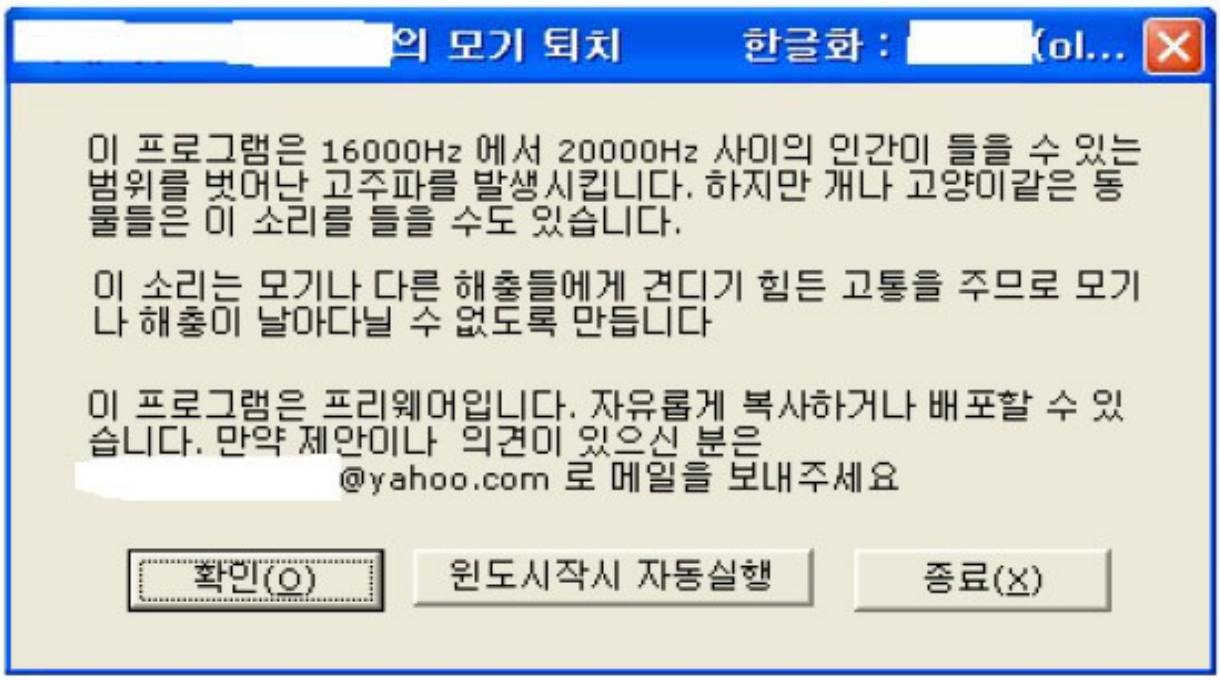
가장 주된 주제는 저의 론술에 대한 이야기였는데 ___동기의 중언은 동기님의 도움을 받는 것이라고 합니다.
그래서 동기님의 넓으신 안목으로 이 론술의 부족을 메꾸어 주었으면 합니다.
다시금 동기님께 감사한 마음을 전하고 싶군요.

더운 날씨에 무리하지 마시고 항상 건강에 관심돌리며 근무하시기를 바라며...
저의 론술을 같이 보내드립니다.
아마 좀 고쳐야 할 것같은데 메일 부탁드리겠습니다.
감사합니다.

Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

장벽 1. 언어 – 한국어 사용자

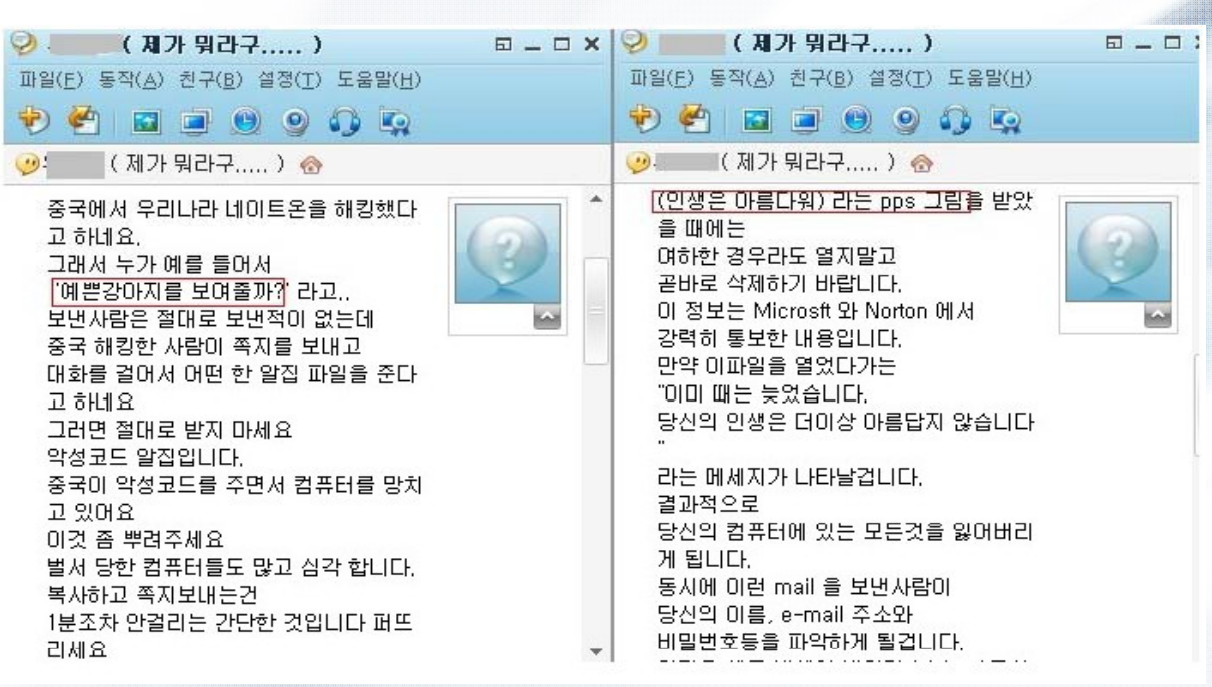
- 한국 사람들이 악성코드 제작에 참가



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

장벽 1. 언어 – 한국어 사용자

- Hoax의 경우 외국어를 한국어로 번역하는 착한(?) 사람들도 있음



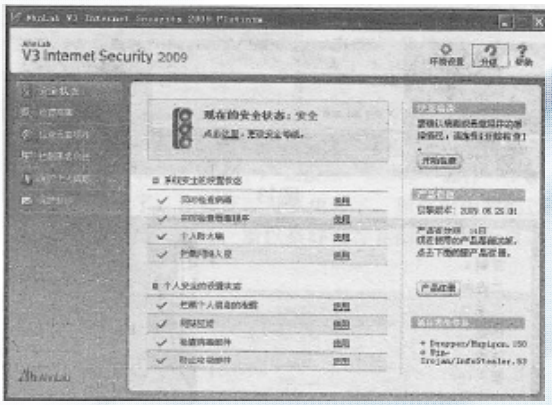
Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

장벽 2. 국산 보안 프로그램

- 국산 보안 프로그램이 널리 이용

- 악성코드 제작자들의 선택
  - 국산 보안 프로그램 방해
  - 업데이트 방해
  - 국산 보안 프로그램 무력화

- 중국에서 국산 보안 프로그램 무력화 연구 지속



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

장벽 3. 사용자 습관

C 군의 일상

'집에 돌아온 C군은 컴퓨터를 켠다. 국산 무료 백신 프로그램인 [**V3라이트**]와 [**알약**]이 자동 업데이트되고 [**네이버**]와 [**다음**]에 접속해 새로운 뉴스를 확인한다. 인터넷에 올라온 이슈를 찾다가 동영상을 보기 위해 [**액티브X컨트롤**]을 설치했다. 이후 [**싸이월드**]와 [**페이스북**] 방명록을 살펴 본 후 [**트위터**]와 [**미투데이**]에 간단히 글을 남긴다. [**웹하드**]에서 동영상과 프로그램 몇 개를 다운로드 하면서 [**네이트온**]을 켜고 친구들과 대화한다. 다운로드가 완료된 동영상은 [**곰플레이어**]로 감상한다. 함께 받은 프로그램은 [**알집**]으로 압축 해제 후 실행해 본다. 리포트를 위해 [**한글**]을 실행한다.'

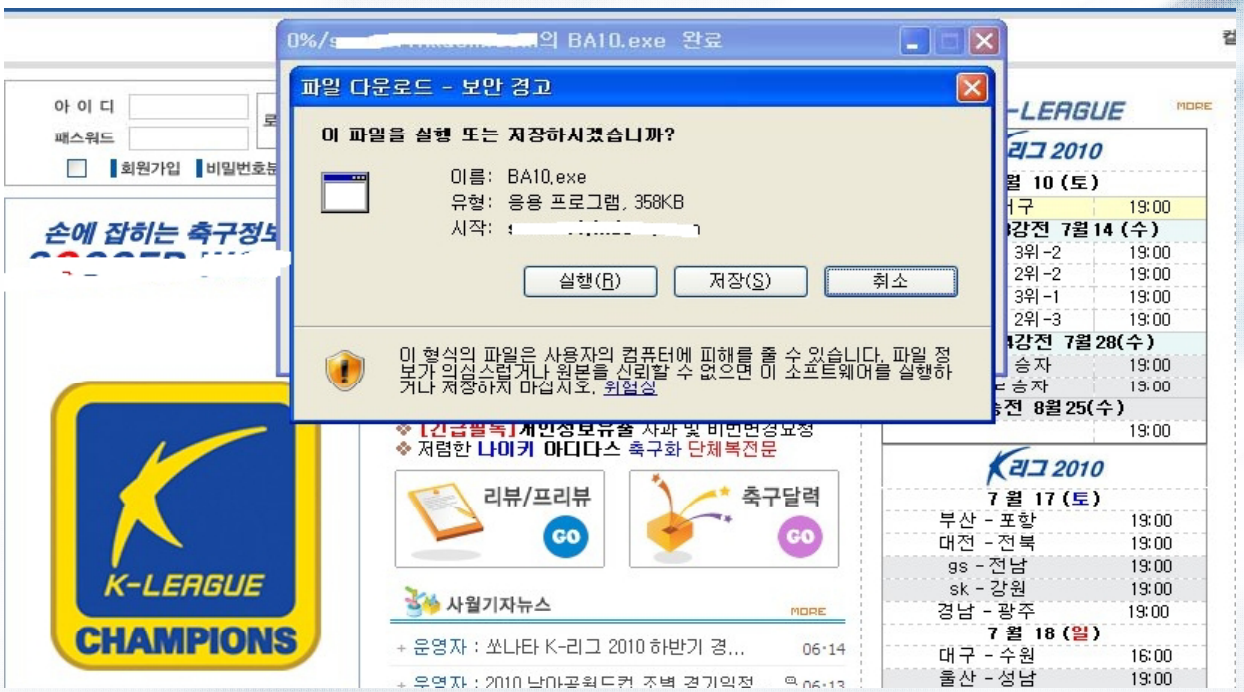
→ **악성코드 제작/배포자들은 국내 사용자들의 컴퓨터 사용 습관을 알아야 함**

Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved.

5. 국내 환경 이용

국내 환경 이용 – 1. 국내 서비스

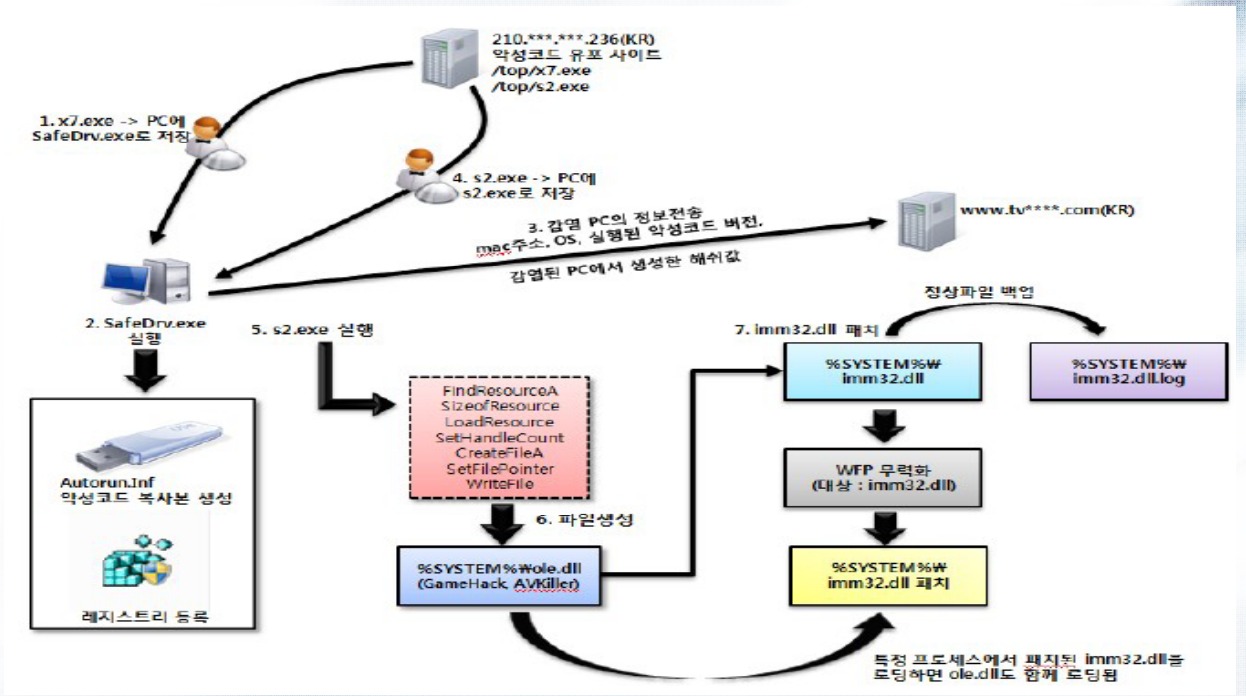
국내 홈페이지
– 악성코드 유포 경로



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 – 1. 국내 서비스

국내 홈페이지
– 악성코드 유포 경로



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 – 1. 국내 서비스

국내 메일 및 블로그
– 악성코드 유포 경로

http://mfiles.naver.net/a77193465c0762de94/20100419_193_blogfile/[illegible]_1271608290971_HMxyMd_exe/Server.exe?type=

http://mfiles.naver.net/1b8e07b4a1fdff230bee8bb0806[illegible]/20100516_37_[illegible]/zero__2_1273947109356_7WADhy_

http://mfiles.naver.net/e174fd475a6a6bdaf41077447690e0983e619311/[illegible]/zero__2_1273575597025_5IKDAO_

http://mfiles.naver.net/1d8801b2a7f9f9250de88aba82641665c79c6980fc/[illegible]/alskg123_1272866981333_Aw8lc9

http://mfiles.naver.net/0ddb39ecf6adc2775b44/20100419_54_blogfile/[illegible]_1271608746918_KEmDBS_exe/Server.exe?type=

http://mfiles.naver.net/2bfd1fcad28be455771e/20100419_191_blogfile/[illegible]_1271670202818_mm1K67_exe/Server.exe?type

http://cfile240.uf.daum.net/attach/[illegible]

http://mfiles.naver.net/5ecb42f2e0b9ba664eabcef9c12f5b2586d22dc893/20100511_227_cafefile/[illegible]127_NnYu0%B9%F6%B1%D7.exe?type=attachment

http://mfiles.naver.net/1d8801b2a7f9f9250de88ab982641863c19c628cfa/[illegible]/alskg123_1272866981333_Aw8lc9

Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 – 1. 국내 서비스

국내 메일 및 블로그

[안내] 악성코드가 포함된 파일 첨부 제한

조회 4844

10.07.07 15:12 주소복사

안녕하세요.

네이버 블로그 서비스 운영팀입니다.

7월 7일, 악성코드가 포함된 첨부파일의 사용을 일부 제한하는
'악성코드 해시필터링 시스템'이 적용됩니다.

이에 따라 한국인터넷진흥원(KISA) 등에서 제공하는 최신 악성코드 해시 값을 포함한 파일은
아래와 같이 파일 업로드 등 블로그 내에서의 일부 이용이 제한됩니다.

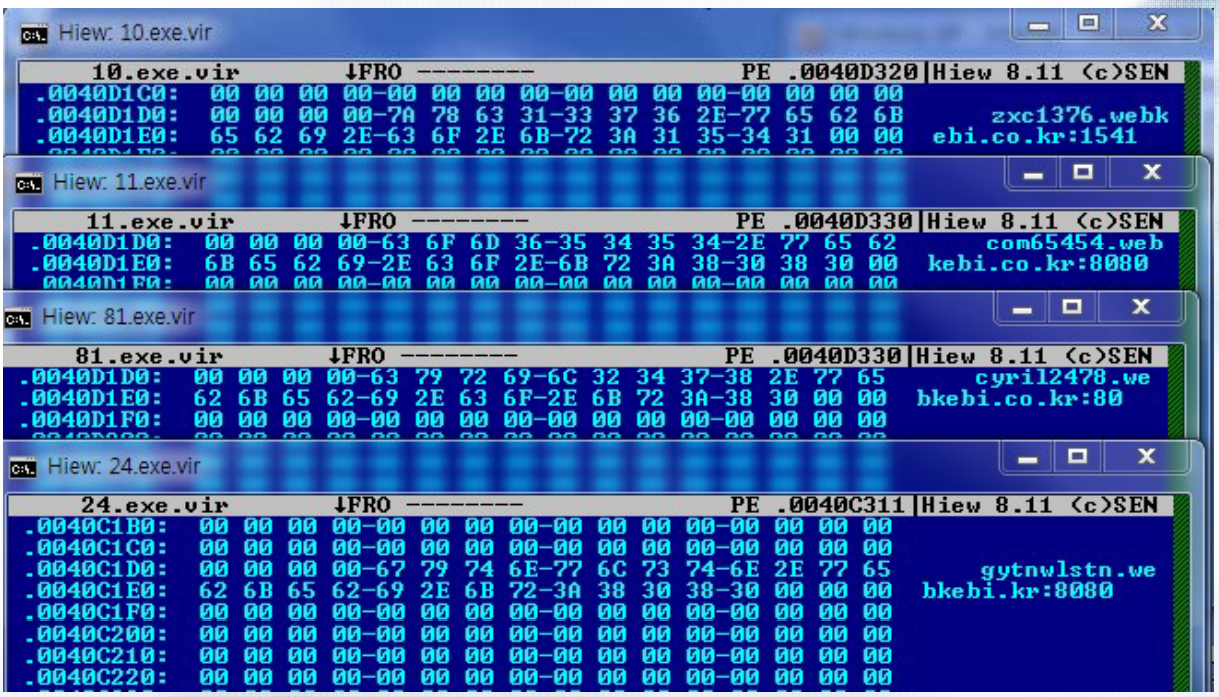
1. 게시물에 파일 등록시

- 신규로 업로드되는 모든 파일에 해시 필터링 시스템이 적용됩니다.
- 내블로그(메모로그 포함) > 스마트에디터 >첨부파일에서 악성코드가 포함된 파일은 업로드 하실 수 없습니다.
- 악성코드로 감염된 파일은 백신 프로그램으로 치료하신 후 다시 첨부하시기 바랍니다.

Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 - 1. 국내 서비스

국내 다이나믹 DNS
- DDoS 공격 명령을 내리는 C&C 서버로 이용



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 - 1. 국내 서비스

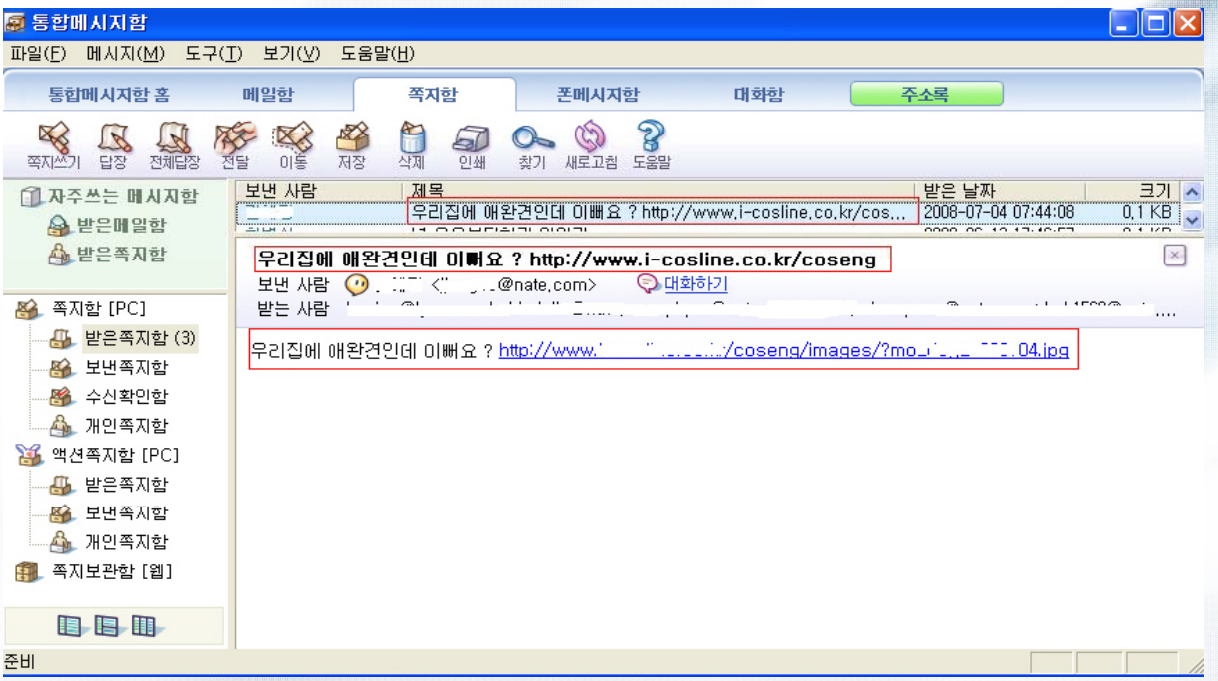
액티브 X 컨트롤
- 비정상적으로 액티브 X 컨트롤 사용이 많음
- 사용자들이 큰 의심 없이 액티브 X 컨트롤 설치

Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 – 1. 국내 서비스

네이트온

- 메신저 사기 등에 이용

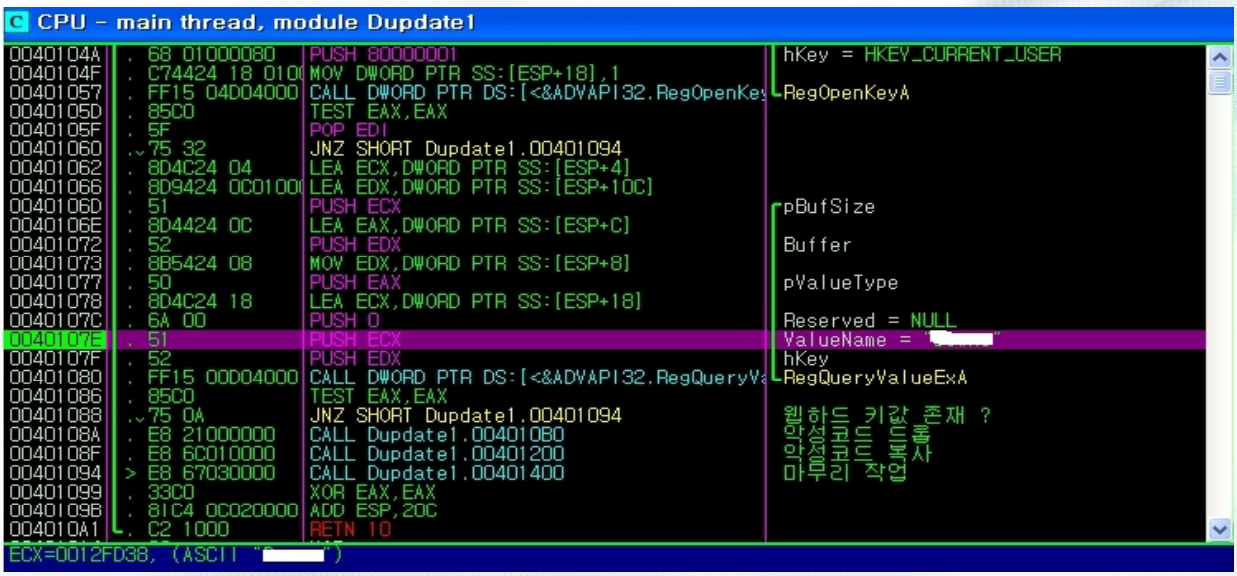


Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 – 1. 국내 서비스

웹하드

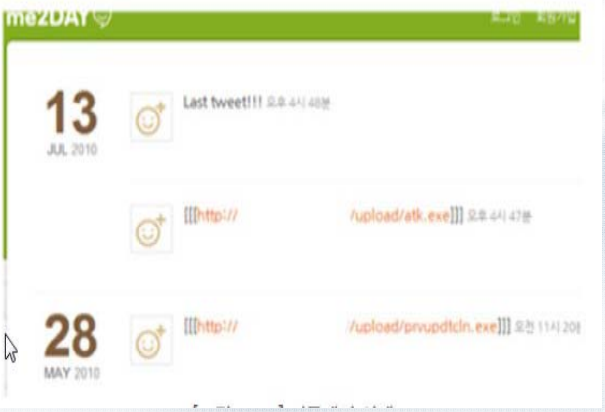
- 주요 악성코드 배포 경로
- 7.7 DDoS 공격 때 이용
- 공격자는 웹하드를 통해 악성코드를 배포하며 웹하드 서비스 업체를 해킹해 업데이트 파일을 악성코드로 교체

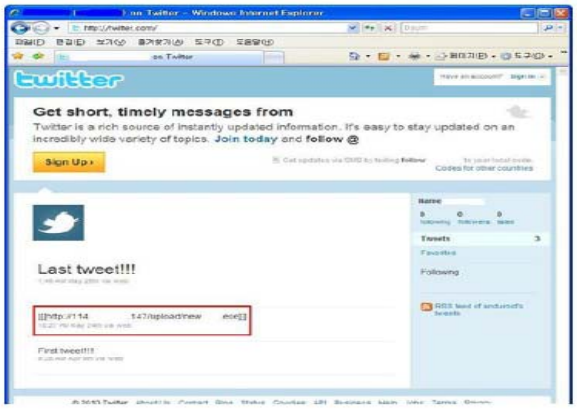


Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 – 1. 국내 서비스

소셜 네트워크 시스템 (SNS)
- Dropper/Twibot.494080, Win-Trojan/Agent.101376.DG
- 미투데이, 트위터 C&C 서버로 이용

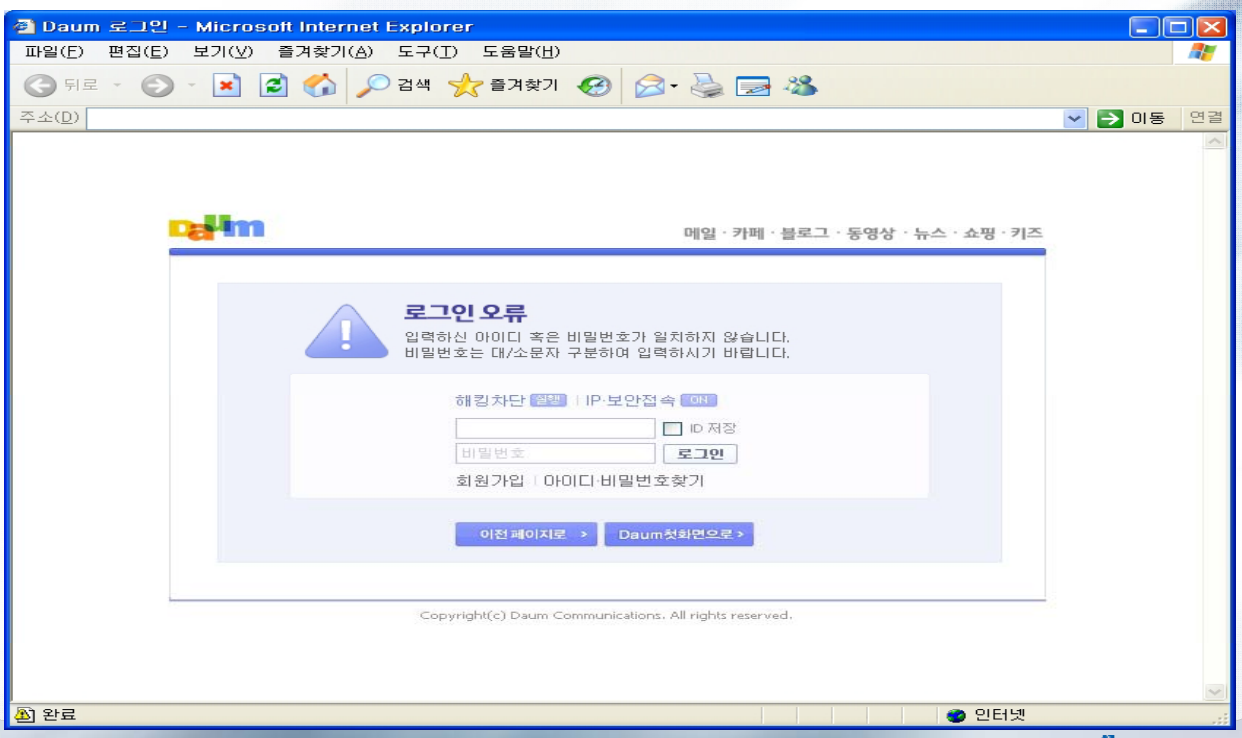




Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 – 2. 정보 유출

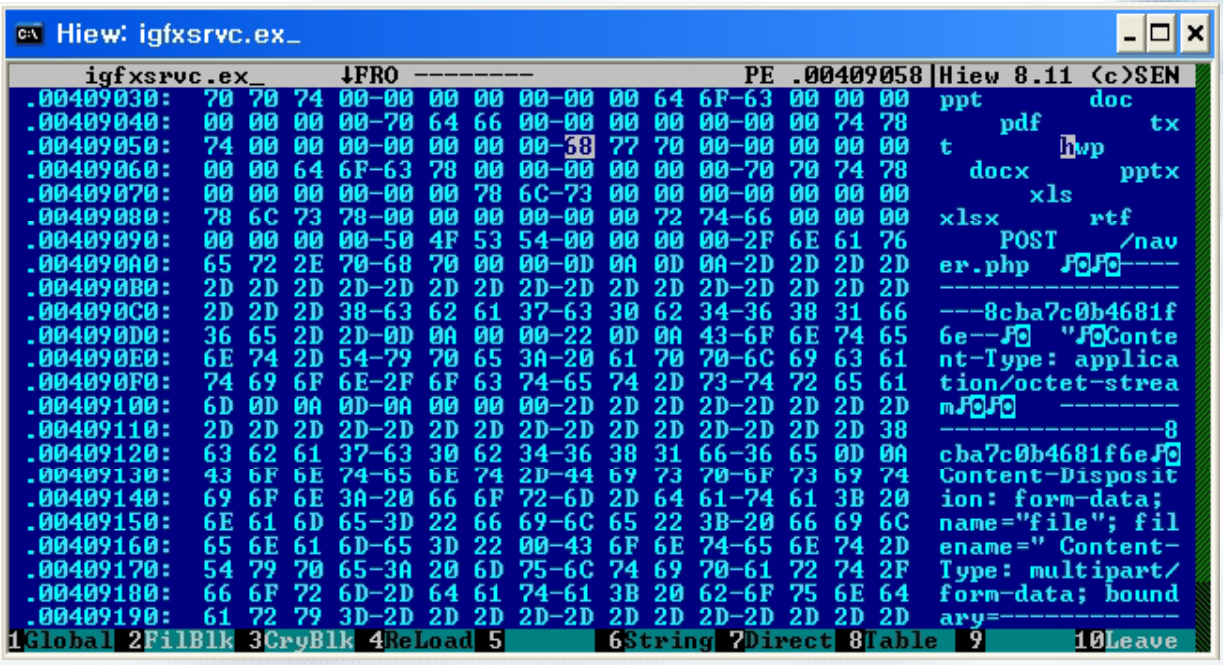
포털/메신저/온라인 게임 계정 탈취
- 가짜 포털 로그인 페이지로 유도



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 – 2. 정보 유출

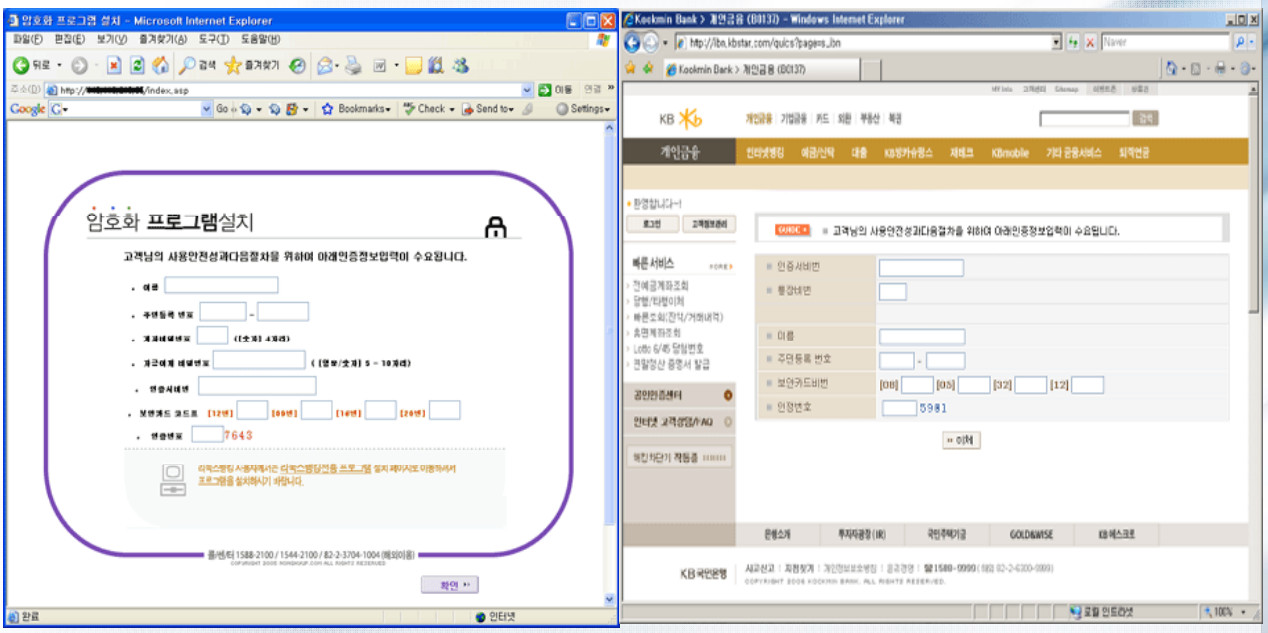
문서 파일 유출
- HWP 파일을 유출하는 Win32/Autorun.worm.49152.AH
- 기업 정보를 빼내기 위한 악성코드로 추정



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 – 2. 정보 유출

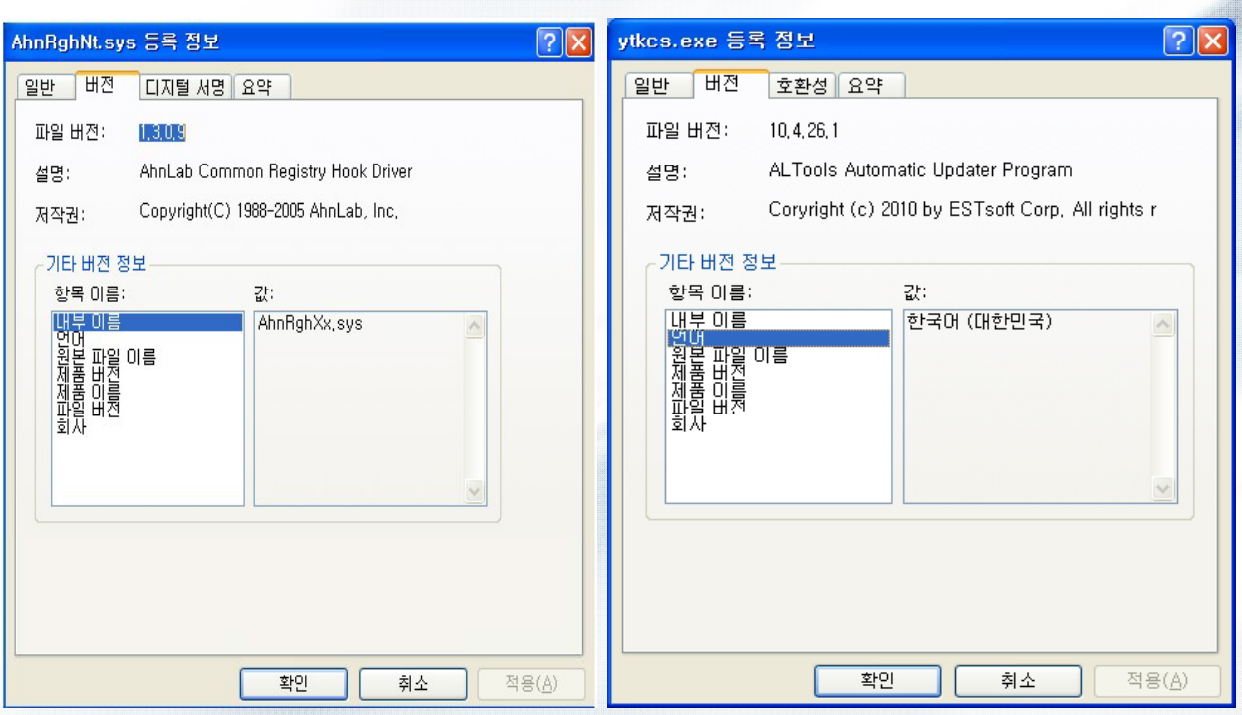
금융 정보 유출
- 국내에서는 [공인인증서] + [보안카드] 정보를 알아야 함
- 2007년 이후 새로운 변형이 등장하고 있지 않음



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

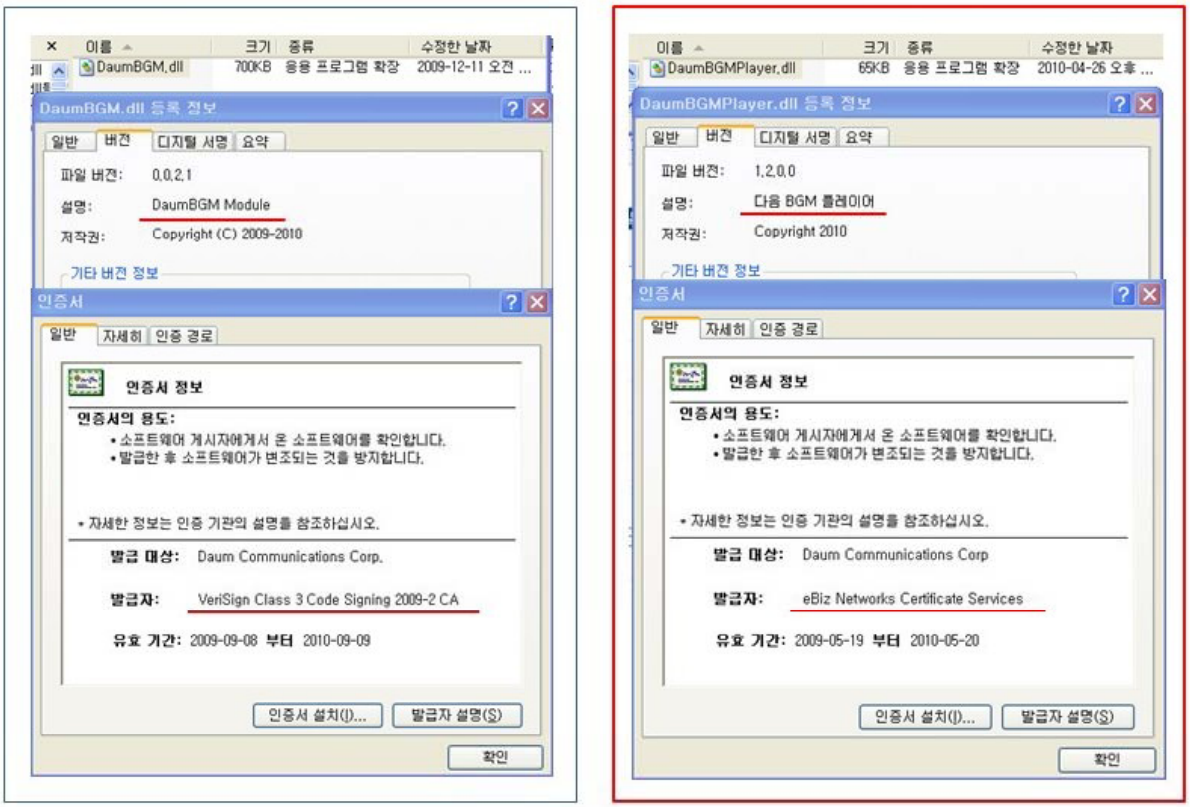
국내 환경 이용 – 3. 유명 프로그램 가장

국내 유명 업체 및 프로그램과 유사한 파일 이름 혹은 등록 정보 이용



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

국내 환경 이용 – 3. 유명 프로그램 가장



Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

6. 향후 전망

안철수연구소

향후 전망

1) 중국 악성코드 제작자들의 노력 : 한국인/한국용 악성코드 제작지

We provide DDOS program for Korean.it is used on attack web server,websites.
Price 5000 CNY for 1 year.(about 800 USD)Use paypal,or Western Union for payment.Contain update server and technical guidance.

상품소개

본 소프트웨어는 막강한 액티비 연결기능, 상대방의 컴퓨터가 어디에 있던지 자유롭게 다룰수 있습니다.
또한 DDOS / KEY LOGGER / WINDOWS REMOTE 기능을 사용하실수 있습니다.
사용법 또한 간단하므로 아무런 전용지식 없어도 사용이 가능합니다.
현재 중국,미국,유럽,러시아 등 나라에서 판매 되고 있는 제품 입니다.
본 제품은 한국 고객님을 위해서 한국어 버전으로 제작되었습니다.
또한 본사에서는 본 제품을 구매하신 VIP고객님에게는 24시간의 에프터마켓 서비스를 해드립니다.

Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved.
안철수연구소

향후 전망

2) 번역기 발전
- 한국어를 몰라도 공격 용의

3) 국내 프로그램 취약점 이용
- 현재는 주로 공개 게시판 취약점 이용
- 현재 국내 프로그램 취약점 정보는 해외에서 거래 안됨
- 국내에 널리 사용되는 프로그램에 대한 취약점 공격 시도 예상

4) 주변국의 변화
- 일본과 관계 악화
- 러시아 악성코드 제작자들이 아시아로 눈 돌린다면 ?!

5) 국내 악성코드 제작자들 동향
- 현재는 기업 형태로 애드웨어/스파이웨어 제작 위주

- ‘악성코드 제작자들은 국내 환경에 빠르게 적응’
- ‘나아가 국내 환경을 적극적으로 이용하기 시작’

-> 보안업체도 일반 사용자들의 인터넷 습관을 이해하고 연구해야 함

Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

Question ?

Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved. 안철수연구소

AhnLab

The Joy of Care-Free Your Internet World

ASEC Threat Research

http://blog.ahnlab.com/asec/
http://core.ahnlab.com

Ahn 안철수연구소

Copyright (C) AhnLab, Inc. 1988-2010. All rights reserved.

AhnLab, the AhnLab logo, and V3 are trademarks or registered trademarks of AhnLab, Inc.,
in Korea and certain other countries. All other trademarks mentioned in this document are the property of their respective owners.